Criptología Simétrica Encriptado-Autenticado

Castro Lechtaler, Antonio[1, 2]; Cipriano, Marcelo[1,3]; García, Edith[1],
Liporace, Julio[1]; Maiorano, Ariel[1]; Malvacio, Eduardo[1], Pazo Robles María Eugenia[1].

[1]Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática.
Facultad de Ingeniería del Ejército -FIE. Universidad de la Defensa Nacional - UNDEF
[2] CISTIC/FCE - Universidad de Buenos Aires.
[3] Departamento de Ciencia y Tecnología, Universidad Nacional de Quilmes UNQ.

{acastro@, marcelocipriano}@fie.undef.edu.ar,
{edithxgarcia; jcliporace; maiorano; edumalvacio; eugepazorobles}@gmail.com

RESUMEN

Con este proyecto se propone investigar dentro de la criptografía simétrica, aquellos algoritmos de clave secreta que encriptan y autentican datos al mismo tiempo, logrando así confidencialidad y autenticidad (además de integridad) de los mensajes que se transmiten..

Nos orientaremos en el estudio de algunos modelos de algoritmos presentados en el concurso Cifrado Autenticado: Seguridad, Adaptabilidad y Robustez (CAESAR) y en la competencia NIST Lightweight Cryptography (Criptología liviana, que incluye encriptado autenticado e integridad) .

Analizaremos en cada caso, las características de diseño de los algoritmos presentados en los mencionados concursos y estableceremos una serie de criterios que es necesario tener en cuenta a la hora de garantizar en un mismo esquema de cifrado de clave simétrica, seguridad, simplicidad y velocidad (Security, Simplicity, Speed S^3).

Este conjunto de técnicas nos permitirá establecer un marco de referencia para el diseño y para la evaluación (a través del criptoanális) del nuevo paradigma para el desarrollo de algoritmos criptográficos simétricos.

Palabras Clave

Criptología Simétrica, Cifrado Autenticado,Cifrado Autenticado con Datos Asociados.

.

CONTEXTO

En el marco de la carrera de grado de Ingeniería en Informática, el posgrado en Criptografía y Seguridad Teleinformática, y de la Maestría de Ciberdefensa que se dictan en la Facultad de Ingeniería del Ejército (FIE) "Gral. Div. Manuel N. Savio" (EST), Universidad de la Defensa Nacional (UNDEF) se llevan adelante tareas de I+D+i por parte del Grupo de Investigación en Criptología y Seguridad Informática (GICSI).

GICSI depende del Laboratorio de Investigación en Técnicas Criptográficas y Seguridad Teleinformática (CriptoLab) perteneciente al Laboratorio Informática (InforLab). Y está conformado por docentes investigadores, profesionales técnicos y alumnos de dicha área.

1. INTRODUCCIÓN

Quizás las dos propiedades fundamentales que debe garantizar la criptografíaía de clave simétrica son la *confidencialidad* (privacidad) y la *autenticidad* (e *integridad*) de los datos que se transmiten a través de canales inseguros. Estas dos características han sido tradicionalmente estudiadas, formalizadas e implementadas por separado[1-2], a través de primitivas criptográficas diferentes (por ejemplo: un algoritmo simétrico en modo CBC para confidencialidad y un CBC MAC para autenticación). Sin embargo tal separación raras veces aparece en la práctica. Por el contrario, en

la gran mayoría de las aplicaciones la autenticidad resulta acompañar a la confidencialidad. Por lo tanto, el problema de alcanzar privacidad y autenticidad simultáneamente con un mismo esquema de cifrado de clave secreta requiere un análisis profundo, exhaustivo y sistemático.

Para tal fin, Bellare y Rogaway (e independientemente Katz y Yung) propusieron en el año 2000 un enfoque formal para solucionar este problema [3-4]. Al mismo tiempo Bellare y Namprempe investigaron la seguridad combinando un esquema de cifrado convencional y una MAC para alcanzar un encriptado autenticado AE [5]. Poco después, aparecieron modelos orientados AE de clave secreta: OCB (2001) [6], CCM (2002)[7-8], y GCM (2004)[9]. La relevancia de eficientes AE en aplicaciones en el mundo real, implicó la estandarización de varios esquemas: el modo CCM en IEEE 802.11i, IPsec ESP e IKEv2; el modo GCM aparece en NIST SP 800-38D; el modo EAX está especificado en ANSI C12.22; e ISO/IEC 19772:2009 tiene seis esquemas AE (cinco diseños orientados AE y un método de composición genérica). En particular el AE se utiliza para evitar lo que se denomina chosen ciphertext attack, donde un atacante puede solicitar a un oráculo que descifre un paquete cifrado y así poner en riesgo todo el criptosistema.

Luego de esta nueva tendencia de diseño de esquemas de AE, surgieron varias cuestiones relativas a la seguridad: errores en las pruebas para medir el nivel de fortaleza, claves débiles, TAGs de tamaño corto y también problemas en la performance e implementación de los algoritmos en diferentes aplicaciones. Una serie creciente de problemas ocasionaron lo que se calificó como *"Desastres"* de la criptografía simétrica [10]. Por otro lado si bien se pueden implementar dos primitivas como las que ya existen para el cifrado y otra para generar una MAC, existe la necesidad de lograr eficientemente realizar ambas operaciones en un mismo esquema de cifrado, implementando un algoritmo y algún modo de operación que realice ambas operaciones y se ajuste a las necesidades de por ejemplo: la transmisión de datos, como ser redes de datos con Pc´s y gran ancho de banda y por otro lado pequeños dispositivos de hardware como los que se usan en IoT(*Internet of Things*) .

Todo esto marcó la necesidad de investigar aún más en el campo del Cifrado Autenticado, y motivó en 2013 hacer la convocatoria de AE CAESAR[11] y en 2015 NIST Lightweight Cryptography[12]. Así se abrió un nuevo campo de investigación que incluye resultados en técnicas de criptoanálisis, diseño y construcción de primitivas criptográficas, análisis de seguridad como así también nuevos modelos formales de seguridad criptológica.

2. LÍNEAS DE INVESTIGACIÓN y DESARROLLO

Para llevar adelante este proyecto se siguen las siguientes líneas de investigación y desarrollo:

- Estudio de material actualizado, asistencia a Cursos, Congresos y Workshops específicos, profundización en el estado del arte del encriptado autenticado y en los nuevos ataques que se hayan desarrollado para tales modelos.
- Estudio, análisis y selección de esquemas de AEAD de clave simétrica.
- Relevamiento de los métodos de diseño que se aplican a los algoritmos AEAD.
- Estudio de técnicas criptográficas para el diseño de esquemas de cifrado autenticado y cifrado autenticado con datos asociados.

- Implementación en diferentes soportes de los esquemas AE.
- Análisis y conclusiones de los resultados obtenidos.

3. RESULTADOS OBTENIDOS / ESPERADOS

Al realizar el estudio, análisis de las técnicas y herramientas para el diseño de AE y AEAD, se persigue establecer un marco de referencia para el diseño de algoritmos de encriptado autenticado:

- Establecer protocolos y métodos de diseño para tales esquemas de cifrado autenticado.
- Evaluar a través de diferentes técnica criptográficas el nivel de seguridad de las primitivas de AE.
- Desarrollar nuevas y buenas prácticas en el diseño en general de algoritmos de clave simétrica.
- Implementar de manera eficiente los AE en diferentes plataformas.

4. FORMACIÓN DE RECURSOS HUMANOS

Los docentes investigadores del proyecto dictan las asignaturas Criptografía y Seguridad Teleinformática, Matemática Discreta y Paradigmas de Programación I, II y son docentes en las materias Criptología y Criptología Avanzada de la Especialización en Criptografía y Seguridad Teleinformática y de la Maestría en Ciberdefensa Desde esas cátedras se invita a los alumnos a participar. Es por ello que 3 de ellos han demostrado su interés y se han sumado en calidad de colaboradores. En particular, el alumno Leiras, Facundo ha recibido la beca "Estímulo a las Vocaciones Científicas" (EVC) otorgadas por el Consejo Interuniversitario Nacional (CIN) [13].

Se desea destacar que el incremento del Know-How que tendrá el grupo de investigadores a lo largo de la vida del proyecto será una importante y económica Formación de Recursos Humanos en beneficio de sus integrantes y de la institución en la cual desarrollan sus actividades científico-docentes.

Por último y atendiendo a la responsabilidad ética y social que compete a la actividad científica y tecnológica, el Grupo Integrante de este Proyecto de Investigación, ya sea durante su ejecución o por la aplicación de los resultados obtenidos, desea expresar su compromiso a no realizar cualquier actividad personal o colectiva que pudiera afectar los derechos humanos, o ser causa de un eventual daño al medio ambiente, a los animales y/o a las generaciones futuras.

5. BIBLIOGRAFÍA

[1] BELLARE, M.—DESAI, A.—JOKIPII, E.—ROGAWAY, P.: A concrete security treatment of symmetric encryption, in: 54th Annual Symp. on Found. of Comput. Sci.– –FOCS '97, Miami Beach, FL, 1997, IEEE Comput. Soc., 1997, pp. 394–403.

[2] BELLARE, M.—KILIAN, J.—ROGAWAY, P.: The security of the cipher block chaining message authentication code, J. Comput. Syst. Sci. 61 (2000), pp. 362–399.

[3] BELLARE, M.—ROGAWAY, P.: Encode-then-encipher encryption: How to exploit nonces or redundancy in plaintexts for efficient cryptography, in: Advances in Cryptology—ASIACRYPT '00 (T. Okamoto, ed.), 6th Internat. Conf. on the Theory and Appl. of Cryptology and Inform. Security, Kyoto, Japan, Lecture Notes in Comput. Sci., Vol. 1976, Springer, Berlin, 2000, pp. 317–330.

[4] KATZ, J.—YUNG, M.: Unforgeable encryption and chosen ciphertext secure modes of operation, in: Fast Software Encryption—FSE '00 (Schneier, B. ed.), 7th Internat. Workshop—FSE '00, New York, NY, USA, 2000, Lecture Notes in Comput. Sci., Vol. 1978, Springer, Berlin, 2001, pp. 284–299.

[5] BELLARE, M.—NAMPREMPRE, C.: Authenticated encryption: relations

among notions and analysis of the generic composition paradigm, in: Advances in Cryptology– –ASIACRYPT ’00 (T. Okamoto, ed.), 6th Internat. Conf. on the Theory and Appl. of Cryptology and Inform. Security, Kyoto, Japan, Lecture Notes in Comput. Sci., Vol. 1976, Springer, Berlin, 2000, pp. 531–545.
[6] ROGAWAY, P.—BELLARE, M.—BLACK, J.—KROVETZ, T.: OCB: A block-cipher mode of operation for efficient authenticated encryption, in: Proc. of the 8th ACM Conf. on Computer and Comm. Security ACM—CCS ’01, ACM New York, NY, USA, 2001, pp. 196–205.
[7] DWORKIN, M.: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. NIST Special Publication 800-38C, Gaithersburg, 2004.
[8] WHITING, D.—HOUSLEY, R.—FERGUSON, N.: Counter with CBC-MAC (CCM). IETF RFC 3610 (Inform). Sep.2003.
http://www.ietf.org/rfc/rfc3610.txt
[9] MCGREW, D. A.—VIEGA, J.: The security and performance of the galois/counter mode (GCM) of operation, in: Progress in Cryptology—INDOCRYPT ’04 (A. Canteaut et al., eds.), 5th Internat. Conf. on Cryptology in India, Chennai, India, 2004, Lecture Notes in Comput. Sci., Vol. 3348, Springer, Berlin, 2004, pp. 343–355.
[10] BERNSTEIN, D. J.: Cryptographic competitions: Disasters, https://web. archive.org/web/20130418063008 /http://cr.yp.to/talks/2013.03.12/slides.pdfhttps://competitions.cr.yp.to/disasters.html (consultada 1-3-20).
[11]https://competitions.cr.yp.to/caesar.html (consultada 1-3-20).
[12]https://csrc.nist.gov/projects/lightweight-Cryptography (consultada 1-3-20).
[13]http://evc.cin.edu.ar/informacion (consultada el 2/3/20).